Dès que vous introduisez votre carte d'identité électronique dans le lecteur, vous dévoilez bon nombre de données personnelles sans le savoir.

LA CARTE D'IDENTITÉ ÉLECTRONIQUE

Ma vie sur une puce

On a dénombré, ces derniers mois, près de deux millions de déclarations fiscales introduites au moyen de tax-on-web avec, d'ordinaire, la carte d'identité électronique comme sésame. D'ici la fin de l'année, tout Belge devra être muni de ce type de carte d'identité, qui ouvrira la voie à moult possibilités, mais aussi à une kyrielle de dangers.

Vincent NAESSENS et Bart DE DECKER

Fin 2009, tout Belge de plus de douze ans sera doté d'une carte d'identité à puce. Elle permettra de s'identifier électroniquement, de s'authentifier, d'apposer une signature digitale sur des documents électronique. Mais elle ne remplacera pas pour autant toutes les cartes qui encombrent le portefeuille. Sans compter qu'une utilisation trop intensive peut s'avérer néfaste.

ASSURANCES ET CAMBRIOLEURS

La carte contient divers fichiers comportant des données d'identification et d'adresse, pouvant être lues dès que l'on introduit le rectangle de plastique dans un lecteur. Cette affichage n'est pas protégé, ce qui signifie qu'il n'est pas nécessaire de pianoter un code pour en prendre connaissance. Sur le site web des autorités, on trouve des logiciels qui en permettent la lecture. Cette fonction de la carte sert souvent à traiter plus rapidement les données concernant les personnes (comme le nom, l'adresse, la photo) aux guichets d'enregistrement, dans les hôtels ou chez le notaire, par exemple. Il faut aussi décliner son identité électronique pour avoir accès à certains parcs de conteneurs, et parfois cela permet de savoir sur quel compte facturer les frais. Même si la carte d'identité électronique peut éviter les files d'attente interminables, il faut en user avec prudence. Car, dès que l'on introduit cette plaquette dans le lecteur, cela dévoile nombre d'informations personnelles, comme le numéro national. Ce numéro d'identification unique permet de relier quantité d'informations entre elles. Exemple: une chaîne de magasins peut se servir de ce numéro pour établir le comportement de consommateur de chaque client. Un agent d'assurances peut relier toutes les polices d'un client à son numéro d'identification. En outre, les prestateurs de services échangent de plus en plus de données. Si l'agent d'assurances et la chaîne commerciale échangent leurs profils, les personnes ayant un mode de vie malsain pourraient voir augmenter leur prime d'assurance.

Il se peut que, pour l'enregistrement, seul le nom soit important. Pourtant, d'autres données, comme la photo ou l'adresse, s'affichent. Il est donc capital d'avoir confiance en la personne ou dans l'institution qui souhaite consulter les données d'identification. Posez-vous la question: Est-ce que cela m'ennuie que telle personne, telle institution, ait accès à mes données d'identification (adresse et photo comprises)? Si tel est le cas, mieux vaut éviter l'utilisation de la carte.

Un courtier peut présenter un contrat, mais envoyer en douce une version adaptée pour signature

En outre, il faut aussi avoir confiance dans l'ordinateur auquel le lecteur de cartes est connecté. Un pc sans programme antivirus et antispyware à jour risque d'être rapidement infecté par un virus s'il est connecté à internet. Les programmes nuisibles peuvent se frayer un accès illimité aux données personnelles d'un individu et les transférer à n'importe quel autre ordinateur. Ainsi, les centres de fitness et de sauna envisagent de plus en plus d'utiliser la carte d'identité électronique à l'entrée. Si un spyware est actif sur leur ordinateur, installé volontairement ou par inadvertance, les infos sur la clientèle, dont l'adresse, peuvent être transmises à des organisations criminelles. Ces dernières sauront donc que le client sera absent de chez lui pendant plusieurs heures: l'occasion rêvée de visiter son domicile.

Il n'est assurément pas recommandé de s'identifier à l'aide d'une carte d'identité électronique si la sécurité n'est pas assurée. En effet, le fichier d'identification peut être lu sur tout poste de travail PC ou portable. Les renseignements apparaissant sur l'écran peuvent être copiés vers une autre carte à puce. Ainsi, un habitant de Remouchamps pourrait se présenter dans le parc à conteneurs de Gesves avec une carte d'identité copiée d'un habitant de cette dernière commune, pour se débarrasser de beaucoup plus de déchets. D'accord, ce cas de figure ne pose peut-être pas de problème capital. Néanmoins, l'identification à l'aide d'une carte d'identité électronique pour se forger un accès aux zones critiques d'une centrale nucléaire est peu souhaitable.

LE FISC

L'authentification électronique est souvent utilisée lors de la connexion à des sites internet comme tax-on-web et remplace des procédures complexes avec mots de passe. Lorsqu'il s'authentifie, l'utilisateur prouve qu'il est le propriétaire de la carte d'identité. Ce qui se fait en plusieurs étapes. D'abord, le serveur envoie une demande d'authentification vers le poste de travail. Cette demande est transférée vers la

Qu'est-ce qui figure sur une carte d'identité électronique?

FICHIER D'IDENTIFICATION

- Nom et prénom
- Numéro national
- Nationalité
- Date et lieu de naissance
- Sexe
- Numéro de la carte
- Numéro de la puce
- Adresse
- Photo
- ...

CERTIFICAT D'AUTHENTIFICATION

- Nom et prénom
- Numéro national
- Nationalité
- Numéro de série
- Clé publique
- ...

carte d'identité électronique. Puis, un nombre d'opérations cryptographiques sont effectuées sur la carte avec une clé privée. Cette clé ne peut pas s'afficher et, par conséquent, ne peut être copiée. Avant que la carte puisse effectuer ces opérations, il faut d'abord encoder un code pin. Finalement, le résultat des opérations cryptographiques retourne vers le serveur (web), avec le certificat d'authentification. Ainsi, le serveur web peut vérifier l'authenticité de l'utilisateur. Le certificat d'authentification se trouve sur la puce et contient un nombre de renseignements personnels (voir encadré).

L'authentification électronique permet aux utilisateurs d'accéder à quantité d'informations personnelles, comme des données financières (déclarations d'impôts et fiches de paie), des données conservées sur les individus dans le registre national (comme le permis de conduire, la situation familiale). Et ces renseignements n'iront qu'en augmentant. Pour résumer, il suffira de pianoter le code pin une seule fois. Ensuite, il sera possible de se connecter sans code à d'autres sites web, tant que la carte reste dans le lecteur.

Le code pin rend l'authentification plus sûre que l'identification. Toutefois, là aussi, la vigilance est de mise. Un programme malveillant sur le pc peut détecter si l'on a déjà tapé le code pin. Si tel est le cas, ce programme peut se connecter, à votre insu, à des serveurs web comme tax-on-web ou myminfin (où l'on trouve des données financières comme les fiches de paie), récupérer des renseignements personnels et les transférer.

Là aussi, il est capital d'avoir entière confiance dans le poste de travail où l'on se connecte. Ce n'est certainement pas toujours le cas des ordinateurs publics. En outre, il ne suffit pas de sécuriser son propre pc. Il faut aussi avoir confiance dans le prestataire de services qui demande l'authentification. Se connecter à des sites web douteux, qui proposent des réductions irréalistes, n'est pas recommandé. Non seulement cela peut provoquer la récupération des données d'identification sur la carte elle-même, mais aussi la perte de renseignements personnels dans les banques de données des autorités.

UNE SIGNATURE NUMÉRIQUE

On peut aussi employer la carte d'identité électronique pour apposer une signature digitale. On gagne du temps auprès des services administratifs: plus besoin d'imprimer des documents et de les envoyer par poste ou fax. Le principe est similaire à celui de l'authentification: on envoie une demande vers la carte afin de signer un document de manière digitale. On tape le code pin et le document est signé.

Le problème, ici, c'est que pour signer des documents d'importance comme des contrats, il faut leur ajouter un *timestamp*, une datation fiable. Ce type de *timestamp* indique le moment où le document a été signé. Pour que la datation soit digne de confiance, une tierce partie est exigée, sinon l'utilisateur pourrait ajouter un *timestamp* figurant une date ultérieure et faire retirer sa carte d'identité électronique immédiatement après avoir apposé sa signature, en signalant aux autorités qu'il l'a perdue. Cela lui permettrait de contester la validité du contrat.

Là aussi, il faut être très prudent si l'on s'installe à d'autres postes de travail et qu'il faut fournir le code pin au moyen du clavier. En effet, des logiciels trompeurs peuvent stocker ce code pin. En cela, les cartes d'identité électroniques diffèrent radicalement des cartes bancaires actuelles (où le code pin est encodé, soit sur un terminal fiable, soit sur un appareil pin pad spécial). En outre, les postes de travail non fiables ne fournissent pas d'assurance absolue quant au document que l'on signe. Un courtier peut présenter un contrat mais envoyer en douce une version adaptée vers la carte, pour signature.

LES POSSIBILITÉS SONT-ELLES INFINIES?

La carte d'identité électronique offre quantité de possibilités intéressantes. De nouvelles applications facilitent l'accès à des informations personnelles ou les tâches administratives. Grâce à cette carte, la Belgique est dans le peloton de tête au niveau de la technologie de la carte d'identité électronique en Europe. Pourtant, les possibilités ne sont pas infinies. Il faudra du temps avant de rendre toutes les autres cartes superflues. Tant les concepteurs des applications que les utilisateurs doivent manier la carte d'identité électronique avec circonspection. Comme pour une carte bancaire, l'usage intempestif de cette plaquette risque d'occasionner des dommages privés. L'essentiel est de bien sécuriser le poste de travail et de savoir estimer correctement les circonstances où l'on est prêt à mettre ses renseignements personnels à la disposition de prestataires de services. ■

Le Dr. Vincent Naessens enseigne au département d'ingénierie industrielle de la Katholieke Hogeschool Sint-Lieven à Gand. Il y dispense des cours de systèmes opérationnels et de sécurisation des logiciels. Il mène une étude dans le domaine de la sécurité IT (Information Technology) et de la vie privée.

Le Prof. Bart De Decker enseigne au département des sciences informatiques de la KULeuven. Son étude se focalise sur les technologies favorisant l'anonymat et l'intimité dans l'univers numérique.

Des points à vérifier pour une utilisation en toute sécurité

- Est-ce que les logiciels de sécurité de l'ordinateur sont à jour?
- Peut-on se fier suffisamment à l'ordinateur que l'on va utiliser?
- Peut-on stocker des données personnelles sur cet ordinateur?
- Le prestataire de services est-il fiable?
- Le prestataire de services a-t-il vraiment besoin de mes données pour le service proposé?
- Le prestataire de services peut-il faire mauvais usage de mes données?